

A F F I D A V I T

STATE OF WEST VIRGINIA

COUNTY OF FAYETTE to-wit:

I, JOHN A. REESE, being duly sworn, hereby state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") having been employed since August 2014. I completed nineteen weeks of training at the FBI Academy in Quantico, Virginia. I am currently assigned to the Charleston, West Virginia, Resident Agency of the Pittsburgh Division, and investigate violations of federal law such as, child exploitation and child pornography, including activity pertaining to the illegal production, receipt, distribution and possession of child pornography in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have been the affiant in multiple search warrants for child pornography. I was previously employed with the Jackson Police Department ("JPD") in Jackson, Tennessee. While employed with the JPD, I investigated criminal offenses including, murder, aggravated assault, burglary, gang activity, drug possession and distribution, rape, child abuse, child neglect and domestic violence. I participated in approximately 450 arrests and issued more than 700 citations as a member of

the JPD. In September 2013, I became a certified member of the JPD SWAT team and remained a member until I joined the FBI in August 2014.

#### SUMMARY OF ARGUMENT

2. I make this affidavit in support of an application for a search warrant for the residential property located at 150 Mulford Circle Drive, Mount Hope, West Virginia 25880, more particularly described in Attachment A, the curtilage of the residence including, but not limited to, storage buildings, and other means of storing, concealing, or producing child pornography ("subject premises"), for evidence of a crime, contraband fruits of a crime, other items illegally possessed, and property designed for use, intended for use or used in committing a crime. As set forth below, I have probable cause to believe that such items, as set forth in Attachment B, incorporated herein by reference, currently are within computer(s) and related peripherals, computer media, and other material found in subject premises.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and investigators. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the

facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities of a violation of 18 U.S.C. §§ 2252 and 2252A are presently located at 150 Mulford Circle Drive, Mount Hope, West Virginia 25880.

STATUATORY AUTHORITY

4. This investigation concerns alleged violations of 18 U.S.C. §§ 2252 and 2252A, relating to material involving the sexual exploitation of minors.

- a. 18 U.S.C. § 2252(a)(1) prohibits knowingly transporting or shipping, using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction of minors engaging in sexually explicit conduct.
- b. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct.
- c. 18 U.S.C. § 2252(a)(4) prohibits knowingly possessing or knowingly accessing with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been shipped or transported using any means or facility of

interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means, including by computer, if the producing of such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct.

- d. 18 U.S.C. § 2252A(a)(1) prohibits knowingly mailing, transporting, or shipping any child pornography using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.
- e. 18 U.S.C. § 2252A(a)(2)(A) prohibits knowingly receiving or distributing any child pornography that has been mailed, or using any means or facility or interstate commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
- f. 18 U.S.C. § 2252A(a)(2)(B) prohibits knowingly receiving or distributing any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
- g. 18 U.S.C. § 2252A(a)(3)(A) prohibits a person from knowingly reproducing child pornography for distribution through the mails, or using any means or facility of interstate or foreign commerce in or affecting interstate or foreign commerce by any means, including by computer.
- h. 18 U.S.C. § 2252A(a)(3)(B) prohibits knowingly advertising, promoting, presenting, distributing, or soliciting through the mails, or using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer, any material or purported material, in a manner that reflects the belief or that is intended to cause another to believe, that the material or purported material is or contains a

visual depiction of an actual minor engaging in sexually explicit conduct, or an obscene visual depiction of a minor engaging in sexually explicit conduct.

- i. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

#### DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

- a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).
- c. "Computer" refers to an electronic, magnetic, optical, electrochemical, or other high speed

data processing device performing logical arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. See 18 U.S.C. § 1030(e)(1).

- d. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how

to configure or use computer hardware, computer software, or other related items.

- g. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. It commonly includes programs to run operating systems, applications, and utilities.
- h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.
- i. "Minor" means any person under the age of 18 years. See 18 U.S.C. § 2256(1).
- j. "Peer-to-peer file-sharing" (P2P) is a method of communication available to Internet users through the use of special software. Computers link together through the Internet using this software, which allows sharing of digital files between users on the same network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.
- k. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor engaged in sexually explicit conduct, see 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor engaging in sexually explicit conduct, see 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (i) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether

between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2)(A).

1. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).
- m. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

#### BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

6. Based on my knowledge, training and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is

produced and distributed.

7. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage and social networking.

8. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

10. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to

set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

12. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

13. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such

files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and

computer habits.

#### PEER-TO-PEER FILE SHARING

14. Millions of computer users throughout the world use Peer-To-Peer ("P2P") file sharing networks to share files containing music, graphics, movies and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the Internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

15. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often, however, a user downloading a file receives the entire file from one computer.

16. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred

between computers. Third-party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

17. P2P software users can search the P2P network by entering search terms into their P2P software to generate a list of available files that contain the search terms. For example, a person interested in obtaining child pornography images would open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user then selects from the results the file(s) he/she wants to download. The files are downloaded directly from the computer sharing the file. The downloaded files are stored in the area or directory previously designated by the user and/or the software. The downloaded files will remain in that same location until moved or deleted.

18. Law Enforcement can search the P2P networks to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. When a user on the P2P network offers a file to trade, the P2P software used by law enforcement calculates a "hash value" of the file using a SHA-1 hash. The Secure Hash Algorithm ("SHA") was

developed by the National Institute of Standards and Technology, along with the National Security Agency, as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. A hash is a mathematical function that converts the data that comprises the contents of a file into an alphanumeric value. This value is unique to every file. A person may copy a file and rename it but if it is an exact copy, regardless of the name of the file, it will have the same hash value.

19. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA-1 operation results in the creation of an associated hash value often referred to as a digital signature. By comparing these hash values, one can determine whether two files are identical with a precision that greatly exceeds 99.9999 percent certainty.

20. An investigator can examine the SHA-1 hash values of files being traded on the P2P network and determine if they are the same as the hash value of a file known to be child pornography. The investigator is able to do this by comparing the hash value associated with a file offered on the P2P network with hash values of movies or images of child pornography identified from previous investigations. The use of SHA-1 hash values for the matching of movies and images has proven to be

extremely reliable. The investigator can then verify the contents of the file by viewing a copy of the file that has the same hash value from a library of known and/or suspected child pornography files kept by the investigator.

21. Most P2P programs allow users to designate specific folder(s) as "shared" folders. Any files contained in those specific folders are then made available for download by other users on the same P2P network. P2P software users typically do not "share" all of the files on their hard drive.

#### BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE

22. Your affiant is aware that Sergeant S.D. Snuffer is an investigator with the Kanawha County Sheriff's Department ("Sgt.") and that he has been trained to conduct undercover investigations utilizing RoundUp Ares, a peer-to-peer file sharing network. On November 1, 2015, Sgt. Snuffer queried the RoundUp Ares peer-to-peer file sharing network to obtain a list of IP addresses in West Virginia that were making available for distribution known or suspected files containing child pornography based on SHA-1 values previously identified by law enforcement. On that same date, Sgt. Snuffer identified IP address 75.109.255.143 as making suspected files containing child pornography available for download. Sgt. Snuffer utilized RoundUp Ares to form a direct, single-source connection between his undercover computer and the computer associated with IP

address 75.109.255.143. During the connection, the computer located at IP address 75.109.255.143 transmitted a list of files it had available for public download, which consisted of 44 files that had been previously been identified as containing suspected child pornography. During the connection, Sgt. Snuffer was able to capture the date, time and hash value of each file downloaded from IP address 75.109.255.143.

23. Your affiant reviewed some of the jpeg files associated with IP address 75.109.255.143 and downloaded on November 1, 2015. Three of the downloaded files are described as follows:

- a) FILE NAME: (ptch lolifuck) 4 yr blowjob 2-10(2).jpg  
HASH VALUE: 7VZBNBAAXUAGPF13CVOSCSOVM6AEBGC7 is an image file that depicts a blonde, prepubescent female performing oral sex on an adult male;
- b) FILE NAME: inga ptch 11.jpg HASH VALUE: CSPCIGIZJNJYLOKSEEIB075R4MMUJAIU is an image file that depicts a blonde, prepubescent female lying on her stomach on a bed. She is nude from the waist down and is touching her vagina; and
- c) FILE NAME: inga pthc 08.jpg HASH VALUE: YP2DKNIL35V0G43A3XR6RXHOMBWP34 is an image file that depicts a blonde, prepubescent female sitting in grass. She is nude from the waist down and is spreading her vagina open with her hand. Information appears on the screen of the image indicating that the prepubescent female is six-years-old.

24. On November 1, 2015, Sgt. Snuffer conducted a query of publicly available records located online by an organization known as the American Registry of Internet Numbers and

determined that IP address 75.109.255.143 was assigned to Internet Service Provider Suddenlink Communications.

25. Your affiant is aware that Sgt. Snuffer continued to utilize RoundUp Ares from November 3, 2015 to March 2, 2016 to form a direct, single-source connection between his computer and the computer associated with IP address 75.109.255.143. During the connections, Sgt. Snuffer was able to capture the date, time and hash value of each file downloaded from IP address 75.109.255.143. Your affiant reviewed some of the files associated with IP address 75.109.255.143 and downloaded between November 3, 2015 and March 2, 2016 and those files are described as follows:

- a) FILE NAME: 080yo 0041 hard(3).jpg HASH VALUE: B46YMUEX4Q3MOIWDIWWFHVYUNX21COP6.jpg - downloaded on 12/03/2015, is an image file depicting an adult male standing behind a pre-pubescent female who is leaning over a couch. The two are engaged in sexual intercourse with visible penetration;
- b) FILE NAME: 13y boy and girl fuck and 11y girl fucks 87 bro HASH VALUE: 3LF2GZXL30PG3PN5COWJNLXKD7V21GTS - downloaded on 12/03/2015, is a ten minute and thirty four second video which depicts a male and female minor on a couch. The two begin kissing and removing their clothes, and then touching each other's penis and vagina. The female minor performs oral sex on the male minor, then the two engage in sexual intercourse in multiple positions on the couch. The male minor performs oral sex on the female minor. There is also a second section of the video titled "Suzie and her little brother" which depicts two prepubescent minors, male and female on a couch. The prepubescent female performs oral sex on the

prepubescent male, and then the two remove their clothing. Finally, the prepubescent female and male sit on the couch and touch each other's genitals for several minutes;

- c) FILE NAME: (1)pthc 201523 HASH VALUE: M67HVHOZOOF3ZZEH2U3CQHNSZY6YVA7V - downloaded on 12/08/2015, is a nine minute video which depicts a prepubescent female masturbating. The prepubescent female also performs oral sex on an adult male. The two then engage in sexual intercourse in multiple positions for several minutes;
- d) FILE NAME: Hussyfan - tied-up bath girl 9y (2) HASH VALUE: 2GBL5KNYRLECADSXUE51F51SJAAAR7JG - downloaded on 12/19/2015, is a two minute and one second video which depicts a prepubescent female with her head covered with a towel. She is tied up with each leg raised and separated. An adult male engages in vaginal sexual intercourse with the prepubescent female, as well as anal sex. Information appears on the screen of the video indicating that the prepubescent female is nine years old. The male ejaculates on the stomach of the prepubescent female; and
- e) FILE NAME: Gargosidad pthc&kingpass (173) HASH VALUE: 1MJTVPS25QGDDA1FNU6PN2B5ZHP5FEU2 - downloaded on 01/03/2016, is a four minute video which depicts a nude prepubescent female laying on a bed. An adult male rubs his penis on her vagina until he ejaculates on her vagina and stomach.

26. On December 5, 2015, Sgt. Snuffer faxed an administrative subpoena to Suddenlink Communications via Neustar Inc. requesting basic subscriber information for IP address 75.109.255.143 between the time period November 1, 2015 through December 3, 2016.

27. On December 28, 2015, Suddenlink Communications via

Neustar Inc. responded to the administrative subpoena and advised that on the dates and time requested, IP address 75.109.255.143 was issued to Eddie McKinney with the customer address of 150 Mill Creek Road, Mount Hope, West Virginia 25880. Suddenlink Communications via Neustar indicated that the account was activated on June 29, 2015.

28. On December 4, 2015, the National Center for Missing and Exploited Children ("NCMEC") provided Sgt. Snuffer with an Initial Hash Value Comparison Report which set forth that 10 of the 27 hash values he submitted for comparison are known children.

29. On January 14, 2016, your affiant searched various records indices for information regarding Eddie McKinney and learned that his current address is listed as 150 Mulford Circle Drive, Mount Hope, West Virginia 25880. Eddie McKinney's date of birth is listed as [REDACTED], 1987 and his social security number is listed as [REDACTED]-5589.

30. On January 14, 2016, your affiant traveled to Mount Hope, West Virginia to conduct surveillance. Initially, your affiant was unable to locate 150 Mill Creek Road. Your affiant spoke with an employee at the Post Office in Mount Hope who advised that Eddie McKinney's current address is 150 Mulford Circle Drive, Mount Hope, West Virginia 25880. According to the employee at the Mount Hope Post Office, Old Mill Creek Road is

connected to Old Mulford Circle Drive. Your affiant also contacted a Raleigh County, West Virginia Emergency Center employee who advised that 150 Mill Creek Road, Mount Hope, West Virginia 25508 does not exist as a physical address. Instead, the accurate physical address is 150 Mulford Circle Drive, Mount Hope, West Virginia 25580. The residence located at 150 Mulford Circle Drive, Mount Hope, West Virginia 25580 is more particularly described in Attachment A.

31. On March 9, 2016, the NCMEC provided Sgt. Snuffer with another Initial Hash Value Comparison Report which set forth that 5 of the 9 hash values submitted for comparison are known children.

#### CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

32. Based upon my knowledge, experience, and training in criminal investigations, and the training and experience of other law enforcement officers trained in child exploitation and child pornography investigations with whom I have had discussions, there are certain characteristics common to individuals involved in the possession, receipt and distribution of child pornography:

- a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

- b. Collectors of child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.
- e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Further, it is common for such users to save and

transfer the pornographic images and/or pornographic video of children from one computer to another because the images are generally difficult to obtain securely.

33. Based on the aforementioned facts, an individual utilizing the Internet services registered to address 150 Mulford Circle Drive, Mount Hope, West Virginia 25880, is likely to be a collector of child pornography because: 1) the person downloaded and utilized a P2P network that your affiant is aware is commonly used to share images and videos of children engaged in sexual acts via the Internet; 2) the person was sharing multiple images; and 3) based upon other investigations, user of such P2P software typically only make a small portion of their collection available for sharing. Such activity is indicative that the user of the Internet services registered to address 150 Mulford Circle Drive, Mount Hope, West Virginia 25880 fits the characteristics of a collector of child pornography.

#### SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

34. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magnetic opticals, and others) can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.


35. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software

(operating systems or interfaces, and hardware drives) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

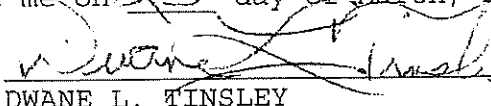
36. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

#### CONCLUSION

37. Based on the foregoing, I submit that evidence and instrumentalities of criminal offenses, namely, violations of 18 U.S.C. §§ 2252 and 2252A are located in the residence at 150 Mulford Circle Drive, Mount Hope, West Virginia 25880, and this evidence, listed in Attachment B is instrumentalities and evidence which is or has been used as the means of committing the foregoing offenses. Your affiant, therefore, respectfully requests that the attached search warrant be issued authorizing the search and seizure of the items listed in Attachment B.

  
\_\_\_\_\_  
JOHN A. REESE  
Special Agent  
Federal Bureau of Investigation

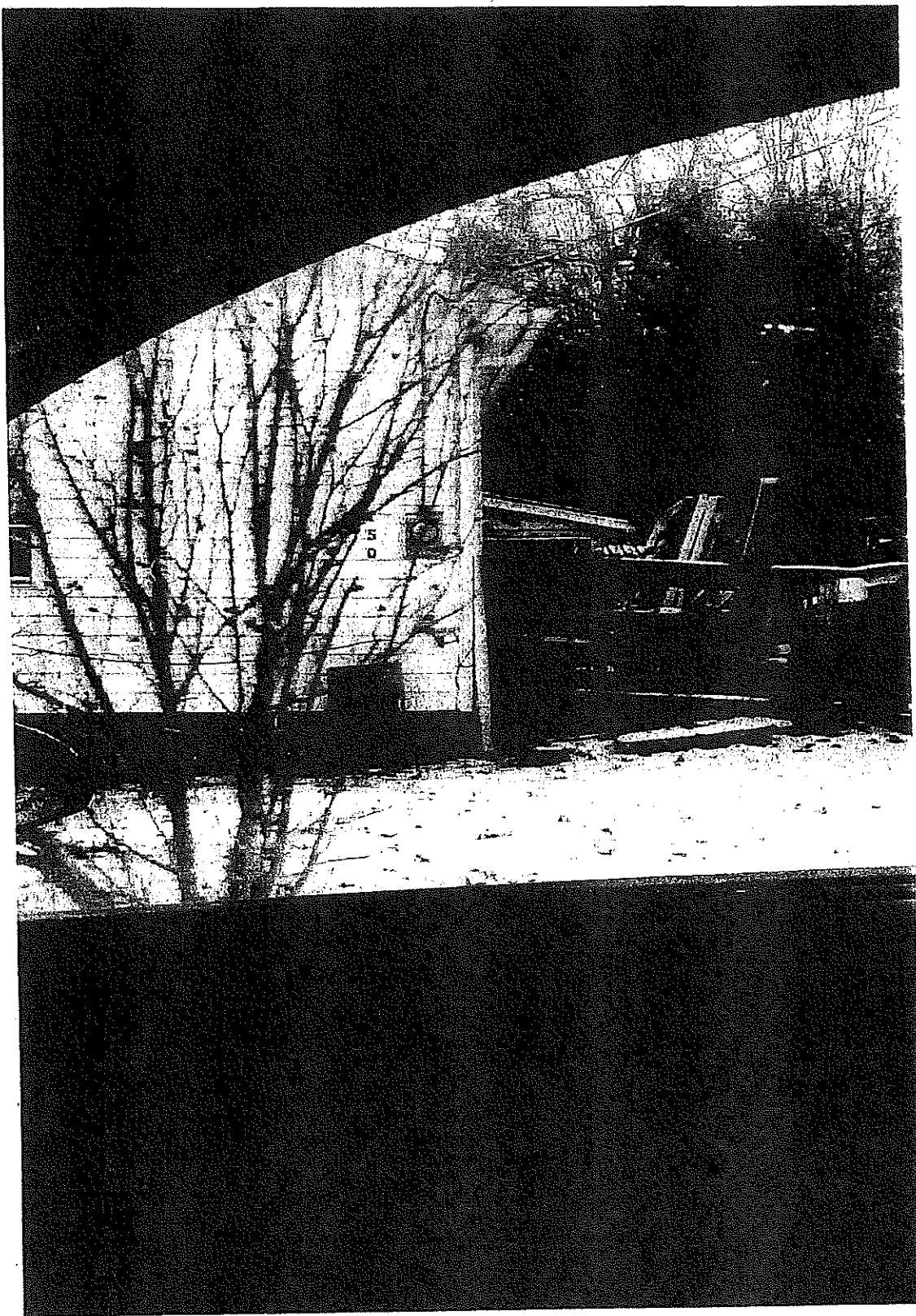
Subscribed and sworn to before me on 23<sup>rd</sup> day of March, 2016.

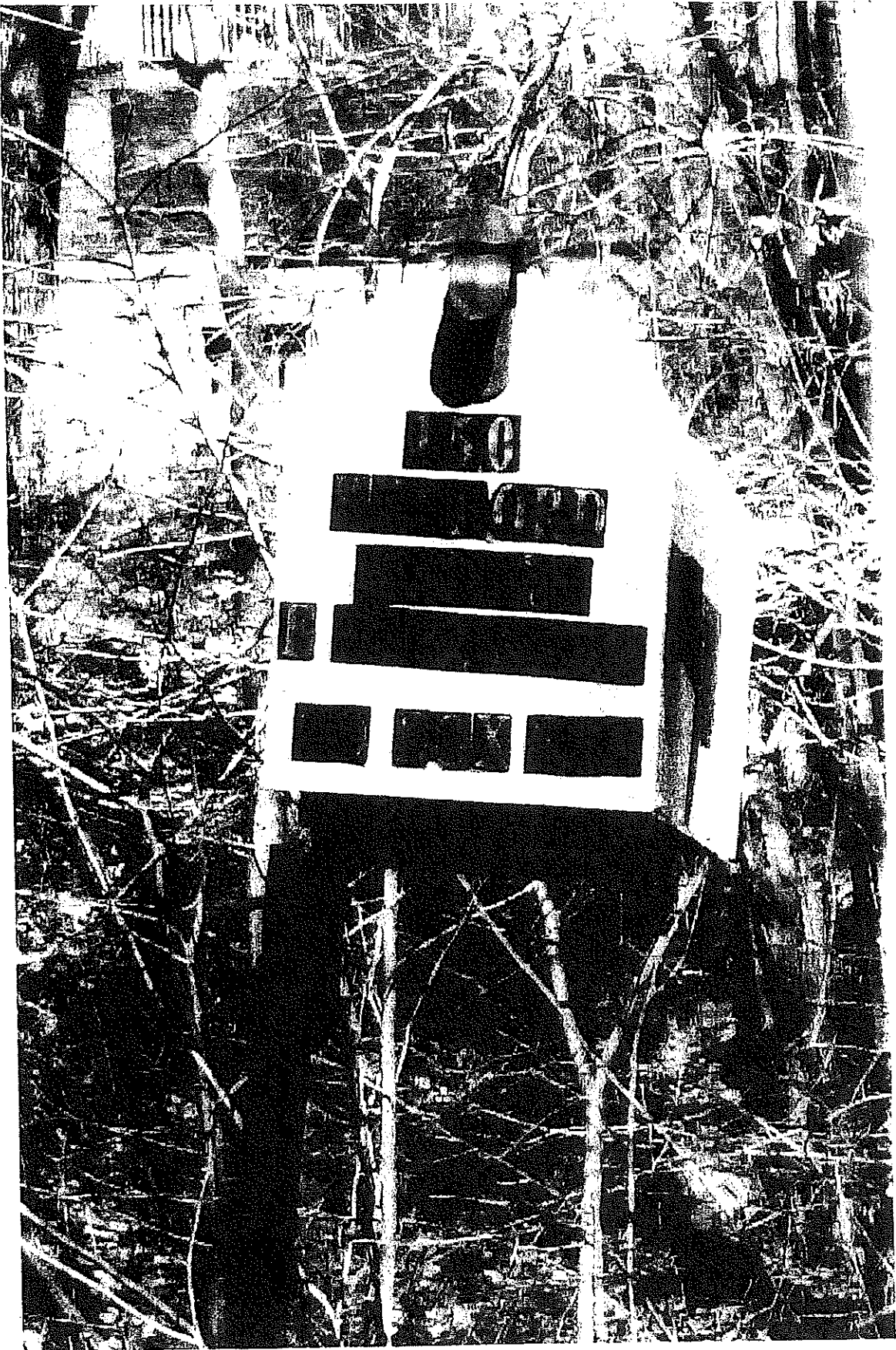
  
\_\_\_\_\_  
DWANE L. TINSLEY  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF WEST VIRGINIA

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The property to be searched ("subject premises") is the entire premises located at 150 Mulford Circle Drive, Mount Hope, West Virginia 25880. The residence is described as a single-story residence with white siding and a visible cinderblock foundation. The numbers 150 are visible on the side of the residence facing the Mulford Circle Drive roadway and next to the utility located at the residence. Wooden porches are attached to the front door and back door of the residence. A black roof covers the residence. A mailbox bearing "150 Mulford Circle E McKinney PO Box 263," is located approximately 750 feet from the subject premises.





ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. Computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Evidence of who used, owned, or controlled the computer(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, accounts of Internet Service Providers.

3. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence, rental or lease agreements, mortgage documents, rental or lease payments and credit card information, including, but not limited to, bills and payment records.

4. Any and all notes, documents, records, computer files or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat

logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), including communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography or membership in online groups, clubs, or services that provide or make accessible child pornography to members.

5. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

6. Any and all cameras, film, videotapes or other photographic equipment.